Certificate Policy
Rabobank PKI 2024

Prepared By: IAM Certificate Management

Rabobank

CERTIFICATE POLICY

Contents

Version control

Version	Date	Reason for change
0.1	25-June-2024	First version, under construction
0.9	9-Sept-2025	Version after review
1.0	23-Sept-2025	Final after review

1 Introduction

This document provides both users and Rabobank – as the Public Key Infrastructure (PKI) operator – with a summary of the binding certification guidelines of Rabobank for the issuance of internal user certificates in the form of a Certificate Policy (CP).

1.1 Overview

This PKI is designed to support validation of claims by current holders of private INRs, in accordance with the records of the organizations that act as Certification Authorities (CAs) in this PKI. The ability to verify such claims is essential to ensuring the unambiguous distribution of these resources [RFC6480].

The structure of the PKI is congruent with the number resource allocation framework of the Internet. The IANA allocates number resources to Regional Internet Registries (RIRs), to others, and for special purposes [RFC5736]. The RIRs, in turn, manage the allocation of number resources to end users, Internet Service Providers, and others.

This PKI encompasses several types of certificates (see [RFC6487] for more details):

- CA certificates for each department distributing INRs and for INR holders
- End-entity (EE) certificates for consumers to validate digital signatures on PKI signed objects

1.2 Document Name and Identification

Title:	Rabobank CP PKI 2024.docx
Classification:	Public
Version:	1.0
Date:	September 2025
Document status:	Draft / in progress
Author:	Erwin Hulst / Certificate Management
O.I.D.:	

1.3 PKI Participants

Note that in a PKI, the term "subscriber" refers to an individual, department or organization that is a subject of a certificate issued by a CA. The term is used in this fashion throughout this document, without qualification, and should not be confused with the networking use of the term to refer to an individual or organization that receives service from an ISP. In such cases, the term "network subscriber" will be used. Also note that, for brevity, this document always refers to PKI participants as organizations or entities, even though some of them are individuals.

1.3.1 Certification Authorities

Department / Team “IDP & CSP Management - On Premise” act as CA for Rabobank.

1.3.2 Registration Authorities

Team Certificate Management act as RA.
RA and CA work in close harmony to facilitate PKI functionality in the widest sense to Rabobank.

1.3.3 Subscribers

These are the departments that are registered to use the API of Rabobank Certificate Management Portal (the RA portal) to request and revoke certificates.

1.3.4 Relying Parties

Entities or individuals that act in reliance on certificates or PKI signed objects issued under this PKI are relying parties. Relying parties may or may not be subscribers within this PKI.

1.3.5 Other Participants

Every organization that undertakes a role as a CA in this PKI is responsible for populating the PKI distributed repository system with the certificates, CRLs, and PKI signed objects that it issues. The organization MAY operate its own publication point, or it MAY outsource this function (see Sections 2.1 and 2.2).

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The certificates issued under this hierarchy are for authorization in support of validation of claims of current holdings of INRs.
Additional uses of the certificates, consistent with the basic goal cited above, also are permitted under this policy. For example, certificates may be issued in support of integrity and access control for the repository system described in Section 2.4. Such transitive uses are permitted under this policy.

1.4.2 Prohibited Certificate Uses

Any uses other than those described in Section 1.4.1 are prohibited under this policy.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is administrated by Certificate Management, IAM Rabobank

1.5.2 Contact Person

The contact information is

Email: Certificate.Management@rabobank.com
Phone: +31 30 215 12 78

1.5.3 CP Approval Procedures

CP is fully managed by department Certificate Management. Any change must be compliant to Rabobank security and cryptography regulations as stated by CISO.
Review will be done after every version change by an authorized security officer (SO). Publication only after approval of the SO.

1.6 Definitions and Acronyms

CA	**Is a trusted entity that issues digital certificates to verify the identity of entities, such as websites, organizations, or individuals.**
CP	**Is a document outlining the rules, procedures, and technical guidelines for issuing, managing, and using digital certificates within a Public Key Infrastructure (PKI)**
CPS	**Certification Practice Statement. A CPS is a document that specifies the practices that a Certification Authority (CA) employs in issuing certificates in this PKI.**
Distribution of INRs	**A process of distribution of the INRs along the respective number hierarchy. IANA distributes blocks of IP addresses and AS numbers to the five Regional Internet Registries (RIRs). RIRs distribute smaller address blocks and AS numbers to organizations within their service regions, who in turn distribute IP addresses to their customers.**

IANA	**Internet Assigned Numbers Authority. IANA is responsible for global coordination of the IP addressing system and AS numbers used for routing Internet traffic. IANA distributes INRs to Regional Internet Registries (RIRs).**
INRs	**Internet Number Resources. INRs are number values for three protocol parameter sets, namely:** • **IP version 4 addresses,** • **IP version 6 addresses, and** • **Identifiers used in Internet inter-domain routing, currently Border Gateway Protocol-4 AS numbers.** **If we are talking about private INR we referring to addresses that are only reachable from within a private Network (like 10.x.x.x or 192.168.x.x number ranges).**
ISP	**Internet Service Provider. This is an organization managing and providing Internet services to other organizations.**
LIR	**Local Internet Registry. In some regions, this term is used to refer to what is called an ISP in other regions.**
NIR	**National Internet Registry. This is an organization that manages the distribution of INRs for a portion of the geopolitical area covered by a Regional Registry. NIRs form an optional second tier in the tree scheme used to manage INRs.**
RA	**Is a trusted entity responsible for verifying the identity of individuals, organizations, or devices before they are granted access to a system or issued a digital certificate, acting as an intermediary between the requester and a Certification Authority (CA) or other granting body.**
RIR	**Regional Internet Registry. This is an organization that manages the distribution of INRs for a geopolitical area.**

2 Publication and Repository Responsibilities

2.1 Repositories

As specified in Rabobank-PKI's Certification Practice Statement.

2.2 Publication of Certification Information

As specified in Rabobank-PKI's Certification Practice Statement.

2.3 Time or Frequency of Publication

As specified in Rabobank-PKI's Certification Practice Statement.

2.4 Access Controls on Repositories

As specified in Rabobank-PKI's Certification Practice Statement.

3 3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The name of the certificate issued (Distinguished Name = DN) must comply with the X.509 standard.

Name	Description
Common Name (CN)	Rabobank customer Identifier
Organizational Unit (OU)	Deprecated
Organization (O)	Cooperatieve Rabobank U.A.
Country (C)	NL
Subject Alternative Names (SAN)	DNS: Any additional CNs
	IP: any IP address directly related to this certificate (mostly used for administrative access)

3.1.2 Need for Names to Be Meaningful

In all cases the Distinguished Name of the certificates must be meaningful and are subject to the rules established in the previous point in this respect.

3.1.3 Anonymity or Pseudonymity of Subscribers

Although subject (and issuer) names need not be meaningful, and may appear "random," anonymity is not a function of this PKI; thus, no explicit support for this feature is provided.

3.1.4 Rules for Interpreting Various Name Forms

None

3.1.5 Uniqueness of Names

There is no guarantee that subject names are globally unique in this PKI. Each CA certifies subject names that MUST be unique among the certificates it issues. Although it is desirable that these subject names be unique throughout the PKI, name uniqueness within the PKI cannot be guaranteed.

However, subject names in certificates SHOULD be constructed in a way that minimizes the chances that two entities in the PKI will be assigned the same name.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of the Private Key

The key pairs for the PKI certificates are stored in certified cryptographic devices of Rabobank and protected by smartcards. Access to this key is only possible by combination of:

- Technical PKI managers
- Functional PKI managers
- Crypto device managers
- Auditors

Which members all have access to a separate part of key or access to the environment.

Protecting and managing private keys of end-user certificates is for responsibility of the end-user. End-user can and may hand over this responsibility to an Rabobank certified and authorized party. Because PKI never accepts or creates a private key for the end-user, the CSR is sufficient prove for possession.

Each CA operating within the context of this PKI MUST require each subject to demonstrate proof of possession (PoP) of the private key corresponding to the public key in the certificate, prior to issuing the certificate. The means by which PoP is achieved is determined by each CA and MUST be declared in the CPS of that CA.

3.2.2 Authentication of Organization Identity

Not applicable
PKI is only available from within Rabobank and will not allow any other organization access.

3.2.3 Authentication of Individual Identity

All access accounts will either verified by:
- Human access: Rabobank HR onboarding process
- NPA / API: based on API onboarding process which is a combination of IAM operations and Certificate Management.

3.2.4 Non-Verified Subscriber Information

A CA MUST NOT include any non-verified subscriber data in certificates issued under this certificate policy except for Subject Information Access (SIA) extensions.

3.2.5 Validation of Authority

Each request will be validate based on:
- Authorized access
- Membership of the Config Admin Group (based on CI number [application, device or other]) for which the certificate is requested.
- Based on ownership of the requested FQDN

Requesters are assumed as representatives for INR holders.

3.2.6 Criteria for Interoperation

This PKI is neither intended nor designed to interoperate with any other PKI.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

The individual identification process shall be the same as in the initial validation.

3.3.2 Identification and Authentication for Re-Key after Revocation

The individual identification process shall be the same as in the initial validation.

3.4 Identification and Authentication for Revocation Request

The individual identification process shall be the same as in the initial validation.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Any employee of Rabobank with access to the computerized network of Rabobank must and should be able to submit a certificate request.
NPA by API can request certificates after an onboarding procedure in which authorization is validated.

4.1.2 Enrollment Process and Responsibilities

To obtain a certificate the following options are available:

1) RCMP (Rabobank Certificate Management Portal), can be used by GUI or API if the appropriate authorizations are met.
2) Autoenrollment. Certain certificates are available for autoenrollment in the Windows domain. Mainly used for laptops, SCCM, and WinRM. If this option is needed contact Certificate.management@rabobank.com
3) Special use cases. Contact certificate.management@rabobank.com for further information.

4.1.3 Time limit for processing the certificate applications

Time limits depends on the type of certificates that are requested:
No time limit:

1) TLS certificates without client authentication
2) Code signing certificates

Human validation (normal office hours):

1) TLS certificates with server and client authentication
2) Client certificates

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

As specified in Rabobank's Certification Practice Statement.

4.2.2 Approval or Rejection of Certificate Applications

Rejection (failure) of applications can be done base on:

1) Automatic checks in RCMP. Example not sufficient key strength
2) Human checks if this is applicable. Example CN is not correct

4.2.3 Time to Process Certificate Applications

See 4.1.3.
In case of human validation within 2 workdays.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

If a CA determines that the request is acceptable, it MUST issue the corresponding certificate and publish it in the PKI distributed repository system via publication of the certificate at the CA's repository publication point (RCMP).

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Issuance of a certificate will be done by mail to the department for which the certificate is requested. This will be determined by looking at the information of the related Config Admin Group in CMDB (ITSM (SM9)).

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Within the timeframe specified in its CPS, the CA places the certificate in the repository and notify the subscriber. Each CA state in its CPS the procedures it follows for publishing of the certificate and notification to the subscriber.

4.4.2 Publication of the Certificate by the CA

Certificates are published in RCMP.
Procedures for publication are defined in the CPS for each CA.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

As stated in Rabobank PKI CPS.

4.5.2 Relying Party Public Key and Certificate Usage

As stated in Rabobank PKI CPS.

4.6 Certificate Renewal

Due to Rabobank policy, every renewal of EE certificates MUST be based on newly generated key-pairs. There see paragraph 4.7.
Exception to this is the half time renewal of a subordinate CA. This will be done in the following way:

1) First half time renewal of CA certificate with same key pair
2) Second half time (full time) re-key of the CA certificate. (4.7)

4.6.1 Circumstance for Certificate Renewal (CA only)

A certificate MUST be processed for renewal based on its expiration date or a renewal request from the subscriber. Prior to the expiration of an existing subscriber's certificate, it is the responsibility of the subscriber to renew the certificate to maintain continuity of certificate usage. If the issuing CA initiates the renewal process based on the certificate expiration date, then that CA MUST notify the holder in advance of the renewal process. The validity interval of the new (renewed) certificate SHOULD overlap that of the previous certificate to ensure continuity of certificate usage. It is RECOMMENDED that the renewed certificate be issued and published at least 1 week prior to the expiration of the certificate it replaces.

Certificate renewal SHOULD incorporate the same public key as the previous certificate, unless the private key has been reported as compromised. If a new key pair is being used, the stipulations of Section 4.7 apply.

4.6.2 Who May Request Renewal

Only the CA certificate holder may initiate the renewal process. The certificate holder MAY request an early renewal, for example, if it expects to be unavailable to support the renewal process during the

normal expiration period. An issuing CA MAY initiate the renewal process based on the certificate expiration date.

4.6.3 Processing Certificate Renewal Requests

Renewal procedures MUST ensure that the person or organization seeking to renew a certificate is in fact the subscriber (or authorized by the subscriber) of the certificate and the legitimate holder of the INR associated with the renewed certificate. Renewal processing MUST verify that the certificate in question has not been revoked.

4.6.4 Notification of New Certificate Issuance to Subscriber

Certificate holder (CA) MUST ensure that all subscribers are aware of the renewal.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Certificate holder (CA) MUST ensure that the new certificates are uploaded to the AIA points en documented.

4.6.6 Publication of the Renewal Certificate by the CA

Certificate holder (CA) MUST ensure that the organisation is aware and updated with the new CA certificate for future usage.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Certificate holder (CA) MUST ensure that all entities are aware of the renewal.

4.7 Certificate Re-Key

This section describes the procedures for certificate re-key. Certificate re-key is the issuance of a new certificate to replace an old one because the key needs to be replaced. Unlike with certificate renewal, the public key is changed.

4.7.1 Circumstance for Certificate Re-Key

Re-key of a certificate SHOULD be performed only when required, based on:

1. knowledge or suspicion of compromise or loss of the associated private key, or
2. the expiration of the cryptographic lifetime of the associated key pair

A CA re-key operation has dramatic consequences, requiring the reissuance of all certificates issued by the re-keyed entity. So it should be performed only when necessary and in a way that preserves the ability of relying parties to validate certificates whose validation path includes the re-keyed entity.

Note that if a certificate is revoked to replace the RFC 3779 extensions, the replacement certificate MUST incorporate the same public key rather than a new key. This applies when one is adding INRs (revocation not required) and when one is removing INRs (revocation required (see Section 4.8.1)).

If the re-key is based on a suspected compromise, then the previous certificate MUST be revoked.

4.7.2 Who May Request Certification of a New Public Key

The holder of the certificate may request a re-key. In addition, the CA that issued the certificate MAY choose to initiate a re-key based on a verified compromise report.

4.7.3 Processing Certificate Re-Keying Requests

The re-key process follows the general procedures of certificate generation as defined in Section 4.3.

4.7.4 Notification of New Certificate Issuance to Subscriber

No additional stipulations beyond those of Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

No additional stipulations beyond those of Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

No additional stipulations beyond those of Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No additional stipulations beyond those of Section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Modification of a certificate occurs to implement changes to selected attribute values in a certificate. This is not allowed in Rabobank PKI and so not possible.
Changing of attributes will only possible by starting a new certificate request.

4.8.2 Who May Request Certificate Modification

Not applicable

4.8.3 Processing Certificate Modification Requests

Not applicable

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable

4.8.6 Publication of the Modified Certificate by the CA

Not applicable

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A certificate MUST be revoked (and published on a CRL) if there is reason to believe that there has been a compromise of a subscriber's private key. A certificate also MAY be revoked to invalidate a data object signed by the private key associated with that certificate. Other circumstances that justify revocation of a certificate is specified in the Rabobank CPS.

Note: If new INRs are being added to an organization's existing distribution, the old certificate need not be revoked. Instead, a new certificate MAY be issued with the new resources. If INRs are being removed or if there has been a key compromise, then the old certificate MUST be revoked (and a re-key MUST be performed in the event of key compromise).

4.9.2 Who Can Request Revocation

As stated in Rabobank PKI CPS.

4.9.3 Procedure for Revocation Request

A subscriber MAY submit a request to the certificate issuer for a revocation. This request MUST identify the certificate to be revoked and MUST be authenticated. The procedures for making the request are described in the CPS for each CA.

A certificate issuer MUST notify the subscriber when revoking a certificate. The notification requirement is satisfied by CRL publication.

4.9.4 Revocation Request Grace Period

A subscriber SHOULD request revocation as soon as possible after the need for revocation has been identified. There is no specified grace period for the subscriber in this process.

4.9.5 Time within which CA Must Process the Revocation Request

As stated in Rabobank PKI CPS.

4.9.6 Revocation Checking Requirement for Relying Parties

A relying party MUST acquire and check the most recent, scheduled CRL from the issuer of the certificate, whenever the relying party validates a certificate.

4.9.7 CRL Issuance Frequency

The CRL issuance frequency is determined by each CA and stated in Rabobank CPS. Each CRL carries a nextScheduledUpdate value, and a new CRL MUST be published at or before that time. Each CA sets the nextUpdate value when it issues a CRL to signal when the next scheduled CRL will be issued.

4.9.8 Maximum Latency for CRLs

The CPS for each CA specifies the maximum latency (overlap time) associated with posting its CRL to the repository system.

4.10 Certificate Status Services

This PKI provisions OCSP for most CAs. These are stated in the Rabobank CPS.

5 Facility, Management, and Operational Controls

Each CA maintains physical security controls for its operation. The physical controls employed for CA operation are specified in Rabobank CPS.

5.1 Physical Controls

5.1.1 Site Location and Construction

Rabobank PKI is hosted in the two available datacenters of Rabobank.

5.1.2 Physical Access

Access to Rabobank datacenters is strictly allowed to only people with a dedicated maintenance role or to people that are based on planned actions registered for that period of time.
Access is always checked and approved by a 24x7 available security desk.
Access to the server floor is always guided by the dedicated team that is responsible for maintenance.

5.1.3 Power and Air Conditioning

Rabobank Datacenters are fully equipped according to Rabobank policy and requirements.

5.1.4 Water Exposure

Rabobank Datacenters are fully equipped according to Rabobank policy and requirements.

5.1.5 Fire Prevention and Protection

Rabobank Datacenters are fully equipped according to Rabobank policy and requirements.

5.1.6 Media Storage

Rabobank Datacenters are fully equipped according to Rabobank policy and requirements.

5.1.7 Waste Disposal

Rabobank Datacenters are fully equipped according to Rabobank policy and requirements.

5.1.8 Off-Site Backup

Rabobank Datacenters are fully equipped according to Rabobank policy and requirements.

5.2 Procedural Controls

5.2.1 Trusted Roles

There are several Roles related to Rabobank PKI

Role	Performed by
Technical Maintenance	IDP & CSP Management - On Premise
Functional Maintenance	Certificate Management
Datacenter	Datacenter management
Audit	AR CITO Cyber, Infrastructure & Cloud
HSM management	EET T4ENG Tech Adherence

5.2.2 Number of Persons Required per Task

Every task is performed by a team.
Access to the servers is depending on the action which is needed.
For accessing the servers and use key material availability of all teams is needed.

5.2.3 Identification and Authentication for Each Role

Every action will be performed by based on a tight scheduled key procedure

5.2.4 Roles Requiring Separation of Duties

See 5.2.1.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Every action need to be done with at least one member of each team (5.2.1) who has followed the procedure before.

5.3.2 Background Check Procedures

Each team member must pass the standard Rabobank background checks.
Besides that he or she must have been assigned to one of the roles mentioned in 5.2.1.

5.3.3 Training Requirements

Each team is responsible to keep skills up to date and is equipped therefor with as development environment.

5.3.4 Retraining Frequency and Requirements

Team members must rotate being at PKI action to keep skills up to date.

5.3.5 Job Rotation Frequency and Sequence

See 5.3.4.

5.3.6 Sanctions for Unauthorized Actions

Every unauthorized action will be forwarded to the responsible manager. Together with the responsible teams impact of this unauthorized action will be determined and suitable measures will be taken to

1) the employee who performed the action
2) prevent further unauthorized actions in the future
3) If needed corrective action

5.3.7 Independent Contractor Requirements

n.a.

5.3.8 Documentation Supplied to Personnel

All documents are kept safe and up to date on the team sites of the different teams.
Only responsible teams (and so employees) have access to these documents.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

All of the following events are recorded as event:

1) Issuing certificate
2) Revocation of certificate
3) Any change in authorization
4) Adding and removing templates (certificate type)
5) Change in templates

Any access to Root CA private key will be logged in an official key ceremony document and recording.

All access to Datacenter to (physically) access the PKI (root) CA closet is controlled, registered and monitored.

5.4.2 Frequency of Processing Log

Planned key ceremonies are once every 6 months.
All other events are logged and monitored continuous.

5.4.3 Retention Period for Audit Log

Logging is kept for 2 years.

5.4.4 Protection of Audit Log

5.4.5 Audit Log Backup Procedures

5.4.6 Audit Collection System (Internal vs. External) [OMITTED]

5.4.7 Notification to Event-Causing Subject [OMITTED]

5.4.8 Vulnerability Assessments

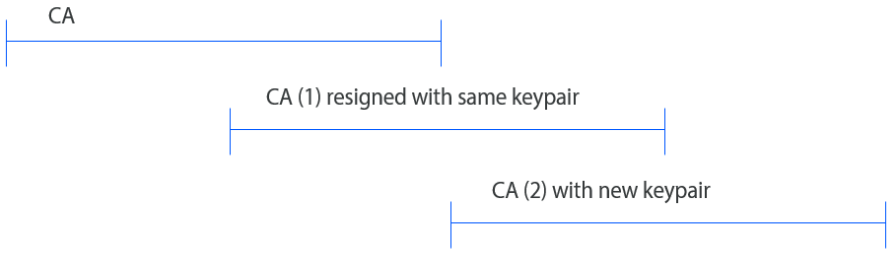
5.5 Records Archival [OMITTED]

5.6 Key Changeover

The following sequence will followed:

1) Every halftime of a CA a renewal with same key will be done
2) Every full time a renewal with new key pair will be initiated.

This results in to the following schema:



Key changeover will always impact the end user. Before the new key will be activated all end users will be informed by CM about the upcoming change and give them sufficient time to update their trust stores.

5.7 Compromise and Disaster Recovery

Any suspicion of compromise will lead to revocation of the related CA. A new CA will be spined up directly.
Depended of the impact a strategy will be chosen regarding timelines of the revocation.

Processes will always be taken with agreement of Management of Rabobank and CISO

5.8 CA or RA Termination

CA termination will be occur in 2 situation:

1) Planned end of service
    a. End of life of the CA certificate (which will result in a renewal)
    b. Decom of CA because of end of service
2) Compromise of key material

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Keypair generation of end-entity (leave) certificates will always be created on customer side. CA or RA will not create any key pair for end-entity certificates. The PKI structure is not equipped for these actions.

6.1.2 Private Key Delivery to Subscriber

n/a

6.1.3 Public Key Delivery to Certificate Issuer

Public key is delivered with a signed CSR by the RA to the Certificate Issuer.

6.1.4 CA Public Key Delivery to Relying Parties

CA public key (certificates) are published at a website (AIA point).
Start point for this is: Rabobank PKI Policies and repository

6.1.5 Key Sizes

Below list is based on the standard security regulation Rabobank follows. Detailed information can be found here: Security Standards and Documents

6.1.5.1 Currently recommended for digital signatures

- For long term (> 1 week < 20 years) digital signatures and signing certificates:
  RSA with a key length of 4096 bits or ECC using secp521r1, using SHA-256 (or larger) as the hashing algorithm2
- For short term <= 1 week valid digital signatures, including client / server certificates and SSH key pairs:
  RSA with a key length of 3072 or 4096 bits or ECC using curves x25519 or secp256r1, using SHA-256 (or larger) as the hashing algorithm.

6.1.5.2 Commonly present in practice and permitted

SHA2 or SHA3 with a hash length of >=256 bits combined with one of ECC or ECDSA using a key length >= 255 bits.

6.1.5.3 Discouraged but still permitted

- RSA or DSA using a key length >= 3072 bits and < 4096 bits for use on long term signatures and >=2048 and < 3072 bits for use on short term signatures, including client / server certificates and SSH key pairs.
- RSA keys > 4096 bits are not recommended for performance and compatibility reasons, opt for 512 bits ECC keys instead.
- SHA2 or SHA3 with a hash length of >=256 bits combined with RSA or DSA using a key length of 2048 bits.
- SHA2 or SHA3 with a hash length of >=224 bits combined with ECC or ECDSA using a key length of 224 bits.

6.1.5.4 Disallowed methods used in digital signatures

- Any signature using SHA-1, MD5 and its predecessors, using RSA and DSA keys with a length < 2048 bits and using ECC / ECDSA keys with a length < 220 bits.

6.1.6 Public Key Parameter Generation and Quality Checking

No extra checking is done than validity on CSR, key validity and signing of this request.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Keys are bound to the certificate. Keys can only be used for the purpose named in the certificate.
The KeyUsage extension bit values employed in PKI certificates are specified in [RFC5280].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Rabobank has specific security regulations on how to handle cryptographic keys.
In case of I=3 and C=3 system must use dedicate security module (HSM hardware or dedicate approved software HSM).

6.2.2 Private Key (n out of m) Multi-Person Control

For CA access to the private key there will be a 3 out of 6 multi person control implemented.

6.2.3 Private Key Escrow

The private key for the production CA will be stored in the cryptographic module. It will be protected from unauthorized use by several measures.

1) Physical access to datacenter
2) Technical team has access to the server but no access key material
3) Access to key material is provisioned by 3 teams who have no access to the server.
4) Every action with use of key material is recorded and audited.

6.2.4 Private Key Backup

Key material is replicated to a dedicated host in the other datacenter.
Keymaterial is protected by HSM stored on several locations spread over the datacenters.

6.2.5 Private Key Archival

See Sections 6.2.3 and 6.2.4.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys will and cannot be transferred from the Cryptographic Modul (HSM), due to the environment configuration of FIPS 140-2 level 3.

The private key is created on the CA with direct connection of the HSM. No export or transfer is needed.

6.2.7 Private Key Storage on Cryptographic Module

At creation the private key is stored in the HSM.

6.2.8 Method of Activating Private Key

Activating the private key for usage is only possible after provisioning a valid quorum of Operator Cards to the HSM.

Operator cards are distributed among 3 teams which all need present to accomplish the validation.

6.2.9 Method of Deactivating Private Key

Deactivation will be done by wiping the HSM and Card set (operator cards and secure world).
Deactivation (destroying) can only take place after confirmation of Certificate Management and IDP & CSP Management - On Premise (with PO and System owner).

6.2.10 Method of Destroying Private Key

See 6.2.9

6.2.11 Cryptographic Module Rating

Fips 140-3 level 3

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CA certificates of Rabobank PKI are not (yet) used for non-repudiation. There is no need for Archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Rabobank intermediate CAs will have a validity period of 5 years.
CA key pairs will be renewed on half of this period (2.5 years). Which will need a redistribution to the trust store of end-users of Rabobank PKI.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Data is protected by HSM which is hosted by Crypto Service team.
CA Servers are installed by <AD Team> according to tier 0 layer standard of Rabobank.

6.4.2 Activation Data Protection

Data is protected by HSM.
Environment is configured according to Tier 0 layer regulations of Rabobank.

Root is protected also by Physical security layer for access datacenter and Server rack. Key material is protected by multiple teams to provide a smartcard to unlock access.

6.4.3 Other Aspects of Activation Data

none

6.5 Computer Security Controls

The TSP takes adequate measures to safeguard availability, integrity and exclusivity.

6.5.1 Technical security requirements

Computer systems are secured against unauthorized access and other threats in an appropriate manner.
All computersystems hosting PKI services are added to security layer 0, which provides special access management, recording of sessions and environment / firewall segmenting.
Penetration testing and risk assessments (yearly) are done for every system

The configuration of the PKI systems are tested/monitored regularly for changes which violates the PKI security policies.

6.5.2 Assignment of security level

The systems and data of the PKI are classified on the basis of current regulations and policy and/or additional Risk Management. This classification is regularly assessed and altered if necessary.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

System development will be done by standard Develop, test, Acceptance process in the dedicated environments.
Implementation will be done with approval and existence of the related teams.

6.6.2 Security Management Controls

Update on OS will be done in sync with the delivery of the updates of Microsoft.
Updates on the offline environment will be done half yearly with renewal of the CRL by manual distribution of the OS updates.

6.6.3 Life Cycle Security Controls

All items are registered in CMDB and will follow and plan the LCM process of hardware and software according to the standard Rabobank LCM process.
PKI will follow and plan OS updates and hardware updates with the dedicated teams responsible for maintenance of the related objects.

6.7 Network Security Controls

Rabobank PKI will operate in Tier 0 security layer with all strict security regulation accordingly. Access is only allowed to those who are involved in technical maintenance PKI supported by a tight change and approval process.

Maintenance access is regulated by strict dual control procedures.

Rabobank Root CA (and policy CA) are hosted as isolated stand-alone.

6.8 Time-Stamping

Rabobank PKI does not use time-stamping.

7 Certificate and CRL Profiles

As specified in Rabobank PKI's Certification Practice Statement.

8 Compliance Audit and Other Assessments

Audits will be executed by an internal Audit department every 2 years.
Findings will be registered and dependent on the level assigned to be solved within the adequate timeframe.

9 Other Business and Legal Matters

9.1 Amendments

9.1.1 Procedure for Amendment

Changes will be first developed and tested in separate/dedicated environments before moving to production.
It can be that security and architecture will be consulted before a change will be installed / configured in production. Decision will be based on considered impact and risk and will be made by product owner and system owner.

9.1.2 Notification Mechanism and Period

Any change which will impact the PKI structure will be communicated 3 months upfront.
Small changes will be communicated and based on the impact determined which timeframe is considered acceptable for the organization. Final decision will be made by the system owner

9.1.3 Circumstances under Which OID Must Be Changed

Any extension or decrease to the OID will create an update to the OID hierarchy.

10 Security Considerations

According to X.509, a certificate policy (CP) is "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements." A CP may be used by a relying party to help in deciding whether a certificate and the binding therein are sufficiently trustworthy and otherwise appropriate for a particular application. This document describes the CP for the Public Key Infrastructure (PKI). There are separate documents (CPSs) that cover the factors that determine the degree to which a relying party can trust the binding embodied in a certificate. The degree to which such a binding can be trusted depends on several factors, e.g., the practices followed by the CA in authenticating the subject; the CA's operating policy, procedures, and technical security controls, including the scope of the subscriber's responsibilities (for example, in protecting the private key), and the stated responsibilities and liability terms and conditions of the CA (for example, warranties, disclaimers of warranties, and limitations of liability).

11 Acknowledgments

-

12 References

12.1 Normative References

Information on RFC 7382 » RFC Editor

12.2 Informative References